Refine Search

Search Results -

Terms	Documents
713.clas.	31118

Database:

US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search:

Refine Search

Recall Text ⇔   Clear   Interrupt

Search History

DATE: Monday, May 14, 2007   **Purge Queries**   Printable Copy   Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
L27	713.clas.	31118	L27
L26	713/162	389	L26
L25	L22 and (decrypting near information or decrypting adj information or decrypting with information)	16	L25
L24	L23 and (decrypting near information or decrypting adj information or decrypting with information)	1	L24
L23	L22 and (sensing with device or sensing near device or sensing adj device)	205	L23
L22	(telecommunication with address or telecommunication near address or telecommunication adj address)	4714	L22
L21	L20 and (telecommunication with address or telecommunication near address or telecommunication adj address)	3	L21
L20	(point and multicast) not @py>1998	797	L20
L19	705/79	270	L19

L18	705/77	235	L18
L17	705/77	235	L17
L16	705/73	88	L16
L15	705/72	220	L15
L14	705/70	122	L14
L13	705/67	731	L13
L12	705/75	684	L12
L11	705/62	242	L11
L10	705/58	430	L10
L9	705/56	324	L9
L8	705/53	497	L8
L7	705/40	1876	L7
L6	705/35	3024	L6
L5	705/34	894	L5
L4	705/33	138	L4
L3	705/23	580	L3
L2	705/21	603	L2
L1	705.clas.	50270	L1

END OF SEARCH HISTORY

```
   L25: Entry 11 of 16                    File: USPT            Feb 28, 2006

US-PAT-NO: 7007166
DOCUMENT-IDENTIFIER: US 7007166 B1

TITLE: Method and system for digital watermarking

DATE-ISSUED: February 28, 2006

INVENTOR-INFORMATION:
NAME                        CITY          STATE    ZIP CODE    COUNTRY
Moskowitz; Scott A.         Miami         FL                   US
Cooperman; Marc             Palo Alto     CA                   US

ASSIGNEE-INFORMATION:
NAME                        CITY    STATE   ZIP CODE    COUNTRY   TYPE CODE
Wistaria Trading, Inc.      Miami   FL                  US        02

APPL-NO: 09/545589   [PALM]
DATE FILED: April 7, 2000

RELATED-US-APPL-DATA:
continuation parent-doc US 08674726 00 19960702 PENDING child-doc US 09545589

INT-CL-ISSUED:
TYPE  IPC           DATE        IPC-OLD
IPCP  H04L9/00      20060101    H04L009/00

INT-CL-CURRENT:
TYPE  IPC           DATE
CIPP  H04 L 9/00    20060101


US-CL-ISSUED: 713/176; 713/168, 380/46
US-CL-CURRENT: 713/176; 380/46, 713/168

FIELD-OF-CLASSIFICATION-SEARCH: 713/176, 713/168, 380/46
See application file for complete search history.

PRIOR-ART-DISCLOSED:

                         U.S. PATENT DOCUMENTS
```

Search Selected | Search ALL | Clear

```
    PAT-NO      ISSUE-DATE            PATENTEE-NAME              US-CL
```

☐	4038596	July 1977	Lee
☐	4200770	April 1980	Hellman et al.
☐	4218582	August 1980	Hellman et al.
☐	4405829	September 1983	Rivest et al.
☐	4424414	January 1984	Hellman et al.
☐	4748668	May 1988	Shamir et al.
☐	4789928	December 1988	Fujisaki
☐	4908873	March 1990	Philibert et al.
☐	4979210	December 1990	Nagata et al.
☐	4980782	December 1990	Ginkel
☐	5073925	December 1991	Nagata et al.
☐	5243515	September 1993	Lee
☐	5287407	February 1994	Holmes
☐	5319735	June 1994	Preuss et al.
☐	5363448	November 1994	Koopman et al.	713/170
☐	5365586	November 1994	Indeck et al.
☐	5379345	January 1995	Greenberg
☐	5394324	February 1995	Clearwater
☐	5408505	April 1995	Indeck et al.
☐	5412718	May 1995	Narasimhalu et al.
☐	5428606	June 1995	Moskowitz
☐	5487168	January 1996	Geiner et al.
☐	5493677	February 1996	Balogh et al.
☐	5530759	June 1996	Braudaway et al.
☐	5568570	October 1996	Rabbani
☐	5606609	February 1997	Houser et al.
☐	5613004	March 1997	Cooperman et al.
☐	5617119	April 1997	Briggs et al.
☐	5636292	June 1997	Rhoads
☐	5640569	June 1997	Miller et al.
☐	5659726	August 1997	Sandford, II et al.
☐	5664018	September 1997	Leighton
☐	5687236	November 1997	Moskowitz et al.
☐	5734752	March 1998	Knox
☐	5745569	April 1998	Moskowitz et al.
☐	5748783	May 1998	Rhoads	382/232
☐	6330672	December 2001	Shur	713/176

OTHER PUBLICATIONS

Alfred J. Menezes, Handbook of Applied Cryptography, 1997, CRC Press LLC, p. 175. cited by examiner

Smith, et al., "Modulation and Information Hiding in Images," Springer Verlag, First International Workshop, Cambridge, U.K., May 30 to Jun. 1, 1996, pp. 207-227. cited by other

Kutter, et al., "Digital Signature of Color Images Using Amplitude Modulation," SPIE-EI97, vol. 3022, pp. 518-527. cited by other

Puate, et al., "Using Fractal Compression Scheme to Embed a Digital Signature into an Image," SPIE-96 Proceedings, vol. 2915, Mar. 1997, pp. 108-118. cited by other

Boney, et al., "Digital Watermarks for Audio Signals," 1996 IEEE Int. Conf. on Multimedia Computing and Systems, Jun. 17-23, Hiroshima, Japan, pp. 473-480. cited by other

Boney, et al., "Digital Watermarks for Audio Signals," Proceedings of EUSIPCO-96, 8th European Signal Processing Conference, Trieste, Italy, Sep. 10-13, 1996, 5 pages. cited by other

Swanson, et al., "Transparent Robust Image Watermarking," Proc. of the 1996 IEEE Int. Conf. on Image Processing, vol. III, 1996, pp. 211-214. cited by other

Swanson, et al., "Robust Data Hiding for Images," 7th IEEE Digital Signal Processing Workshop, Sep. 1-4, 1996, Loen, Norway, pp. 37-40. cited by other

Cox, et al., "Secure Spread Spectrum Watermarkings for Multimedia," NEC Research Institute, Technical Report 95-10, 1995, 33 pages. cited by other

Zhao, et al., "Embedding Robust Labels into Images for Copyright Protection," Proceedigns of the KnowRight'95 Conference, pp. 242-251. cited by other

Kock, et al., "Towards Robust and Hidden Image Copyright Labeling," 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Jun. 1995, 4 pages. cited by other

Langelaar, et al., "Copy Protection for Multimedia Data based on Labeling Techniques," Dept. of Electrical Engineering, Information Theory Group, Delft Univ. of Tech., Delft, The Netherlands, Jul. 1996, 9 pages. cited by other

Van Schyndel, et al., "A Digital Watermark," IEEE International Computer Processing Conference, Austin, TX, Nov. 13-16, 1994, pp. 86-90. cited by other

Van Schyndel, et al., "Towards A Robust Digital Watermark," Second Asian Image Processing Conference, Singapore, Dec. 6-8, 1995, vol. 2, pp. 504-508. cited by other

Tirkel, et al., "A Two-Dimensional Digital Watermark," DICTA'95, University of Queensland, Brisbane, Dec. 5-8, 1995, 7 pages. cited by other

Tirkel, A.Z., "Image Watermarking--A Spread Spectrum Application," ISSSSTA'96, Sep. 1996, Mainz, Germany, 6 pages. cited by other

Ruanaidh, et al., "Watermarking Digital Images for Copyright Protection," IEF Proceedings, vol. 143, No. 4, Aug. 1996, pp. 250-256. cited by other

Hartung, et al., "Digital Watermarking of Raw and Compressed Video," SPIE vol. 2952, EOS Series, Symposium on Advanced Imaging and Network Technologies, Berlin, Germany, Oct. 1996, pp. 205-213. cited by other

Press, et al., "Numerical Recipes in C," Cambridge University Press, 1988, 12. Fourier Transform Spectral Methods, pp. 398-470. cited by other

Pohlmann, Ken C., "Principles of Digital Audio," Third Edition, 1995, pp. 32-37, 40-48, 138, 147-149, 332, 333, 364, 499-501, 508-509, 564-571. cited by other

Pohlmann, Ken C., "Principles of Digital Audio," Second Edition, 1991, pp. 1-9, 19-25, 30-33, 41-48, 54-57, 86-107, 375-387. cited by other

Schneier, B., "Applied Cryptography," John Wiley & Sons, Inc., New York, 1994, particularly the following sections: 4.1 Subliminal Channel, pp. 66-68, 16.6 Subliminal Channel, pp 387-392, Ch. I pp 1-16, Ch. 2 pp 17-41, Ch. 3 pp 42-57, Ch. 12.1 pp 273-275, Ch 14.1 pp 321-324. cited by other

Kahn, D., "The Code Breakers," The Macmillan Company, 1969, particularly the following sections on steganography pp. xiii, 81-83, 513, 515, 522-526, 873. cited by other

Brealey, et al., "Principles of Corporate Finance, Appendix A--Using Option-Valuation Models," 1984, pp. 448-449. cited by other

Copeland, et al., "Real Options: A Practitioner's Guide," 2001, pp. 106-107, 201-202, 204-208. cited by other
Sarkar, M. "An Assessment of Pricing Mechanisms for the Internet--A Regulatory Imperative," presented at MIT Workshop on Internet Economics, Mar. 1995. http://www.press.umich.edu/jep/works/SarkAssess.html on Mar. 12, 2001. cited by other
Crawford, D.W., "Pricing Network Usage: A Market for Bandwidth or Market Communication?" presented at MIT Workshop on Internet Economics, Mar. 1995. http://www.press.umich.edu/jep/works/CrawMarket.html on Mar. 12, 2001. cited by other
Low, S.H., Equilibrium Allocation and Pricing of Variable Resources Among User-Suppliers (1988). http://citeseer.nj.nec.com/366503.html. cited by other

ART-UNIT: 2132

PRIMARY-EXAMINER: Barron, Jr.; Gilberto

ASSISTANT-EXAMINER: Lanier; Benjamin E.

ABSTRACT:

A method for applying a digital watermark to a content signal is disclosed. In accordance with such a method, a watermarking key is identified. The watermarking key includes a binary sequence and information describing application of that binary sequence to the content signal. The digital watermark is then encoded within the content signal at one or more locations determined by the watermarking key.

65 Claims, 0 Drawing figures

L25: Entry 11 of 16   File: USPT   Feb 28, 2006

DOCUMENT-IDENTIFIER: US 7007166 B1
TITLE: Method and system for digital watermarking

Description Paragraph (76):
Bandwidth rights instruments are likely to be highly localized to specific subnets.
Especially since certain types of·connections may be available only from certain
exchanges, and since failure probabilities are likely to vary with specific
hardware, operating systems, and service providers. Additionally, the basic
valuation equations above do not address telecommunications costs across various
types of lines. This problem at least, might be solved by active maintenance of
cost tables, designation codes for types of lines, and the designation of a low
cost standard. The problem of moving rights between exchanges is made more
difficult since supply/demand planning for one exchange will not translate to
another, unless some means for interconnecting exchanges is developed, and exchange
bandwidth planning is global. The race by many parties to link users to the
INTERNET via varying access links (modem) including ISDN, POTs, cable, may further
the need for common bandwidth pricing. What is clear is that the basic structure of
the present invention would facilitate such planning to the benefit of all market
participants: telecoms providers, INTERNET access companies, users and publishers
as well as more general aggregators of content and bandwidth such as, phone
companies, cable companies and satellite companies intending on providing services
across multifarious line types.

CLAIMS:

22. The method of claim 19, wherein said one or more references is selected from
the group consisting of: a encode/decode algorithm which is capable of encoding and
decoding bits of information directly to and from the content signal, a function
which relates the sequence of binary numbers to the content signal; a function
which assesses the frequency content of the content signal before embedding the at
least one watermark; a function which is capable of encrypting and decrypting
information contained in the at least one watermark, and a function which embeds
into the content signal an informational signal which comprises information about
the at least one watermark such that the informational signal may be used to
correct any errors that may have been introduced into the at least one watermark.

   L25: Entry 14 of 16   File: USPT   ·   Feb 26, 2002

US-PAT-NO: 6351640
DOCUMENT-IDENTIFIER: US 6351640 B1

TITLE: Initiating a Telecommunications call to a party based on an identifying
signal wirelessly transmitted by the party or its proxy

DATE-ISSUED: February 26, 2002

INVENTOR-INFORMATION:
NAME   CITY   STATE   ZIP CODE   COUNTRY
DeMont; Jason Paul   Basking Ridge   NJ

ASSIGNEE-INFORMATION:
NAME   CITY   STATE ZIP CODE COUNTRY TYPE CODE
Lucent Technologies, Inc. Murray Hill   NJ   02

APPL-NO: 08/944387   [PALM]
DATE FILED: October 6, 1997

PARENT-CASE:
REFERENCE TO RELATED APPLICATION This is a division of application Ser. No.
08/574,059, filed Dec. 15, 1995, now pending.

INT-CL-ISSUED: [07] H04B 1/38, H04Q 7/32

INT-CL-CURRENT:
TYPE IPC   DATE
CIPS H04 Q 7/22   20060101
CIPS H04 Q 7/38   20060101
CIPN H04 Q 7/32   20060101

US-CL-ISSUED: 455/426; 455/415, 455/460, 455/536, 455/564, 455/566, 455/575,
455/90, 455/351
US-CL-CURRENT: 455/426.1; 455/351, 455/415, 455/460, 455/556.1, 455/564, 455/566,
455/575.9, 455/90.3

FIELD-OF-CLASSIFICATION-SEARCH: 455/403, 455/414, 455/5, 455/426, 455/460, 455/466,
455/500, 455/517, 455/550, 455/556, 455/564, 455/566, 455/568, 455/569, 455/575,
455/91, 455/95, 455/99, 455/100, 455/227, 343/702
See application file for complete search history.

PRIOR-ART-DISCLOSED:

                          U.S. PATENT DOCUMENTS

Search Selected | Search ALL | Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4164025	August 1979	Dubnowski et al.	364/900
☐	4922518	May 1990	Gordon et al.	379/57
☐	4939768	July 1990	Inaba et al.	379/58
☐	4980910	December 1990	Oba et al.	379/355
☐	5020150	May 1991	Shannon	455/343
☐	5097502	March 1992	Suzuki et al.	379/356
☐	5117449	May 1992	Metroka et al.	455/552
☐	5214793	May 1993	Conway et al.	455/517 X
☐	5218629	June 1993	Dumond et al.	379/59
☐	5230073	July 1993	Gausmann et al.	395/600
☐	5276729	January 1994	Higuchi et al.	379/58
☐	5280516	January 1994	Jang	379/57
☐	5307349	April 1994	Shloss et al.	370/85.2
☐	5329578	July 1994	Brennan et al.	379/67
☐	5365516	November 1994	Jandrell	370/18
☐	5412654	May 1995	Perkins et al.	370/94.1
☐	5418845	May 1995	Reeder	379/213
☐	5428678	June 1995	Fitzpatrick et al.	379/201
☐	5566358	October 1996	Obayashi et al.	455/435 X
☐	5668559	September 1997	Baro	343/702
☐	5835861	November 1998	Whiteside	455/466

ART-UNIT: 2683

PRIMARY-EXAMINER: Trost; William

ASSISTANT-EXAMINER: Sobutka; Philip J.

ATTY-AGENT-FIRM: DeMont & Breyer, LLC

ABSTRACT:

A method and apparatus for initiating a telecommunications call. A plurality of beacons (102) are geographically disposed in a telecommunications system (100). Each beacon (102n) radiates an electromagnetic carrier that is modulated with an identifying address (e.g., a telephone number, an Internet address) for an associated terminal. An identifying signal is stored in a memory (206). A controller (208) modulates a carrier with the identifying signal and a transmission element (210) transmits the carrier to allow a communications terminal (104) to

initiate a call to the associated communications terminal (114, 116). A wireless terminal (104a) includes a directional receiver (204). To initiate a call, a user points directional receiver (204) at a beacon. The directional receiver (204) receives the electromagnetic carrier and the wireless terminal recovers the identifying address. Wireless terminal (104) then uses the identifying address to initiates a call, in well-known fashion, to the communications terminal associated with the identifying address.

33 Claims, 15 Drawing figures

L25: Entry 14 of 16   File: USPT   Feb 26, 2002

DOCUMENT-IDENTIFIER: US 6351640 B1
TITLE: Initiating a Telecommunications call to a party based on an identifying
signal wirelessly transmitted by the party or its proxy

Brief Summary Text (11):
Alternative embodiments of the invention provide a method and apparatus for
initiating a telecommunications call (whether voice, video, data or multimedia)
while avoiding many of the costs and restrictions associated with conventional
techniques. Specifically, alternative embodiments of the present invention enable
the initiation of a telecommunications call to a communication terminal (e.g., a
wireless terminal, a wireline terminal, an automatic call distribution system,
etc.) based on the reception of an identifying address (e.g., the telephone number,
the Internet address) of the communications terminal via a directional receiver.

Detailed Description Text (3):
The illustrative embodiment comprises one or more "beacons" (e.g., beacons
102.sub.1, 102.sub.2, . . . , 102.sub.n). Each beacon 102.sub.i advantageously
radiates an electromagnetic carrier that is modulated with data including, among
other things, an identifying signal (e.g., a telephone number, an Internet address)
of an associated communication terminal that is accessible via telecommunications
system 100 and addressable by the identifying signal. Paging transmitter 118 can
provide a signal to a beacon to remotely modify, for example, the identifying
signal for the beacon as described more fully below. The details of where beacon
102.sub.i is located and what information it radiates will be discussed below.

Detailed Description Text (15):
The operation of wireless terminal 104a is as follows. A user points directional
receiver 204 at a beacon to receive the electromagnetic carrier radiated by the
beacon. Directional receiver 204 recovers the identifying signal from the
electromagnetic carrier and provides the identifying signal to processor 202, in
well-known fashion. Processor 202 then provides the identifying signal to radio
208, which uses the identifying signal, in well-known fashion, to initiate a call,
via telecommunications system 100, to the communication terminal associated with
the identifying address.

Detailed Description Text (40):
To facilitate privacy and restrict the number of users who can receive information
radiated by a beacon, the user data, transmissive data and/or identifying signal
radiated by a beacon may be encrypted, in well-known fashion. In such cases,
processor 202 must be capable of decrypting the encrypted information. Processor
202 may be given the cryptographic key via a keypad or penpad, or via
telecommunications system 100.

        L25: Entry 15 of 16   File: USPT   Jan 19, 1999

US-PAT-NO: 5862220
DOCUMENT-IDENTIFIER: US 5862220 A

TITLE: Method and apparatus for using network address information to improve the
performance of network transactions

DATE-ISSUED: January 19, 1999

INVENTOR-INFORMATION:
NAME   CITY   STATE   ZIP CODE   COUNTRY
Perlman; Stephen G.   Mountain View   CA

ASSIGNEE-INFORMATION:
NAME   CITY   STATE   ZIP CODE   COUNTRY   TYPE CODE
WebTV Networks, Inc.   Mountain View   CA   02

APPL-NO: 08/656923   [PALM]
DATE FILED: June 3, 1996

INT-CL-ISSUED: [06] H04L 9/08, ·H04L 9/00

INT-CL-CURRENT:
TYPE IPC   DATE
CIPS H04 M 7/00   20060101
CIPS H04 N 5/00   20060101
CIPN H04 L 29/08   20060101
CIPS H04 L 29/12   20060101
CIPN H04 M 7/12   20060101
CIPN H04 N 7/16   20060101
CIPS H04 L 29/06   20060101
CIPN H04 Q 3/72   20060101
CIPS H04 M 3/487   20060101
CIPS H04 M 3/493   20060101
CIPS H04 N 7/167   20060101

US-CL-ISSUED: 380/21; 380/9, 380/10, 380/49, 380/59
US-CL-CURRENT: 713/162; 348/E5.004, 348/E7.056, 380/251, 380/279, 380/59, 713/155

FIELD-OF-CLASSIFICATION-SEARCH: 380/4, 380/9, 380/21, 380/23, 380/25, 380/49,
380/50, 380/59, 380/10
See application file for complete search history.

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

| Search Selected | Search ALL | Clear |

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4182933	January 1980	Roseblum	380/21
☐	4852151	July 1989	Dittakavi et al.	379/97
☐	4876717	October 1989	Barron et al.	380/25
☐	4922523	May 1990	Hashimoto	379/96
☐	4975944	December 1990	Cho	379/209
☐	4995074	February 1991	Goldman et al.	379/97
☐	5005011	April 1991	Perlman et al.	340/728
☐	5056140	October 1991	Kimbell	380/23
☐	5095494	March 1992	Takahashi et al.	375/10
☐	5241587	August 1993	Horton et al.	379/92
☐	5263084	November 1993	Chaput et al.	379/215
☐	5287401	February 1994	Lin	379/98
☐	5299307	March 1994	Young	395/161
☐	5325423	June 1994	Lewis	
☐	5341293	August 1994	Vertelney et al.	364/419.17
☐	5369688	November 1994	Tsukamoto et al.	379/100
☐	5410541	April 1995	Hotto	370/76
☐	5425092	June 1995	Quirk	379/215
☐	5469540	November 1995	Powers, III et al.	395/158
☐	5488411	January 1996	Lewis	348/8
☐	5490208	February 1996	Remillard	379/96
☐	5538255	July 1996	Barker	
☐	5561709	October 1996	Remillard	379/96
☐	5564001	October 1996	Lewis	
☐	5612730	March 1997	Lewis	348/8

OTHER PUBLICATIONS

Matt Rosoff, Review: "Gateway Destination PC," c/net inc., 2 pages, Feb. 19, 1996.
Robert Seidman, Article: What Larry and Lou Know (That You Don't), c/net inc., 2 pages, Jan. 29, 1996.
Susan Stellin, Article: "The $500 Web Box: Less is More?" c/net inc., 2 pages, 1996.

ART-UNIT: 276

PRIMARY-EXAMINER: Gregory; Bermarr E.

ATTY-AGENT-FIRM: Workman, Nydegger & Seeley

ABSTRACT:

An apparatus and method for using network address information to improve the
performance and increase the functionality of network transactions. is disclosed.
In a client network interface device having a processor and a memory coupled to the
processor, the memory having stored therein sequences of instructions which when
executed by the processor cause the processor to perform the steps of: 1) accessing
a first server over a secure data communication line to obtain a client encryption
key, 2) accessing a second server over an unsecure data communication line to
establish a connection with the second server, 3) encrypting information sent to
the second server over the connection using the client encryption key obtained from
the first server, and 4) decrypting information received from the second server
over the connection using the client encryption key obtained from the first server.
The present invention further includes sequences of instructions which when
executed by the processor cause the processor to perform the steps of, 1)
connecting to an unsecure server over an unsecure data communication line to
perform unsecure portions of a data transaction, 2) disconnecting from the unsecure
server; and 3) connecting to a secure server over a secure data communication line
to perform secure portions of the data transaction.

52 Claims, 16 Drawing figures

L25: Entry 15 of 16   File: USPT   Jan 19, 1999

DOCUMENT-IDENTIFIER: US 5862220 A
TITLE: Method and apparatus for using network address information to improve the
performance of network transactions

Abstract Text (1):
An apparatus and method for using network address information to improve the
performance and increase the functionality of network transactions. is disclosed.
In a client network interface device having a processor and a memory coupled to the
processor, the memory having stored therein sequences of instructions which when
executed by the processor cause the processor to perform the steps of: 1) accessing
a first server over a secure data communication line to obtain a client encryption
key, 2) accessing a second server over an unsecure data communication line to
establish a connection with the second server, 3) encrypting information sent to
the second server over the connection using the client encryption key obtained from
the first server, and 4) decrypting information received from the second server
over the connection using the client encryption key obtained from the first server.
The present invention further includes sequences of instructions which when
executed by the processor cause the processor to perform the steps of, 1)
connecting to an unsecure server over an unsecure data communication line to
perform unsecure portions of a data transaction, 2) disconnecting from the unsecure
server; and 3) connecting to a secure server over a secure data communication line
to perform secure portions of the data transaction.

Brief Summary Text (3):
This invention is in the field of telecommunications, as it relates to the use of
network address information for network transactions.

Brief Summary Text (16):
The present invention is an apparatus and method for using network address
information to improve the performance and increase the functionality of network
transactions. A client network interface device is disclosed as having a processor
and a memory coupled to the processor, the memory having stored therein sequences
of instructions which when executed by the processor cause the processor to perform
the steps of: 1) accessing a first server over a secure data communication line to
obtain a client encryption key, 2) accessing a second server over an unsecure data
communication line to establish a connection with the second server, 3) encrypting
information sent to the second server over the connection using the client
encryption key obtained from the first server, and 4) decrypting information
received from the second server over the connection using the client encryption key
obtained from the first server. The present invention further includes a client
network interface device having a processor and a memory coupled to the processor,
the memory having stored therein sequences of instructions which when executed by
the processor cause the processor to perform the steps of, 1) connecting to an
unsecure server over an unsecure data communication line to perform unsecure
portions of a data transaction, 2) disconnecting from the unsecure server; and 3)
connecting to a secure server over a secure data communication line to perform
secure portions of the data transaction.

CLAIMS:

1. A client network interface device having a processor and a memory coupled to said processor, the memory having stored therein sequences of instructions to be executed by said processor, said instructions comprising:

a first instruction for accessing a first server over a secure data communication line to obtain a client encryption key;

a second instruction for accessing a second server over an unsecure data communication line to establish a connection with said second server;

a third instruction for encrypting information sent to said second erver over said connection using said client encryption key obtained from said first server; and

a fourth instruction for decrypting information received from said second server over said connection using said client encryption key obtained from said first server.

2. A first server having a processor and a memory coupled to said processor, the memory having stored therein sequences of instructions to be executed by said processor said instructions comprising:

a first instruction for receiving a request from a client over an unsecure data communication line to establish a connection with said client;

a second instruction for accessing a second server over a secure data communication line to obtain a client encryption key corresponding to said client;

a third instruction for decrypting information received from said client over said connection using said client encryption key obtained from said second server; and

a fourth instruction for encrypting information sent to said client over said connection using said client encryption key obtained from said second server.